

h

Notice of Allowability

Application No.

09/645,588

Examiner

Beemnet W. Dada

Applicant(s)

ARITA, SEIGO

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to Amendment filed on 06/16/2005.
2. ☒ The allowed claim(s) is/are 1-39.
3. ☒ The drawings filed on 25 August 2000 are accepted by the Examiner.
4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☒ All b) ☐ Some* c) ☐ None of the:
 1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|---|---|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 2. <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 6. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____ |
| 3. <input type="checkbox"/> Information Disclosure Statements (PTO-1449 or PTO/SB/08),
Paper No./Mail Date _____ | 7. <input checked="" type="checkbox"/> Examiner's Amendment/Comment |
| 4. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 8. <input type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| | 9. <input type="checkbox"/> Other _____ |

DETAILED ACTION

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with David Blumenthal Reg. No. 26,257 on 07/21/2005.

The application has been amended as follows: In the claims,

1. (Currently Amended) A secure parameter generating device in an algebraic curve cryptography having the definition expression of $\alpha Y^a + \beta X^b + 1 = 0$, comprising:
 - an input means for receiving two different prime numbers (a, b) specifying degree of complexity of a curve and size (n) of an encryption key to be used;
 - a Stickelberger element computing device for computing a Stickelberger element (ω) in an ab cyclotomic, based on the prime number (a) and the prime number (b);
 - a Jacobian addition candidate value computing device for computing Jacobian addition candidate value j corresponding to the two different prime numbers a and b, and a prime number p corresponding to the Jacobian addition candidate value j, based on the prime number (a), the prime number (b), the size (n) of an encryption key, and the Stickelberger element (ω);

an order candidate value computing device for computing a class H consisting of a plurality of candidate values for order of a Jacobian group of an algebraic curve specified by the prime number a and the prime number b, based on the prime number a, the prime number b, and the Jacobian addition candidate value j;

a security judging device for searching for a candidate value h meeting a security condition such as almost prime number characteristic from the class H, according to the class H;

a parameter deciding device for computing a parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h, of the algebraic curves specified by the prime number a, the prime number b, and the prime number p, based on the prime number a, the prime number b, the prime number p, and the candidate value h; and

an output device for supplying the parameter of the algebraic curve computed by said parameter deciding device to an algebraic curve cryptographic public key system.

18. (Currently Amended) A secure parameter generating method in an algebraic curve cryptography having the definition expression of $\alpha Y^a + \beta X^b + 1 = 0$, comprising the steps of:

a Stickelberger element computing procedure for computing a Stickelberger element ω in an ab cyclotomic, respectively based on two different prime numbers a and b specifying degree of complexity of curve;

a Jacobian addition candidate value computing procedure for computing Jacobian addition candidate value j corresponding to the two different prime numbers a and b , and a prime number p corresponding to the Jacobian addition candidate value j , respectively based on the prime number a , the prime number b , the size n of an encryption key, and the Stickelberger element ω ;

an order candidate value computing procedure for computing a class H consisting of a plurality of candidate values for order of a Jacobian group of an algebraic curve specified by the prime number a and the prime number b , respectively based on the prime number a , the prime number b , and the Jacobian addition candidate value j ;

a security judging procedure for searching for a candidate value h meeting a security condition such as almost prime number characteristic from the class H , according to the class H ; and

a parameter deciding procedure for computing a parameter of an algebraic curve whose order of the Jacobian group is in accord with the candidate value h , of the algebraic curves specified by the prime number a , the prime number b , and the prime number p , respectively based on the prime number a , the prime number b the prime number p , and the candidate value h ; and

supplying said parameter to an algebraic curve cryptographic public key system.

Conclusion

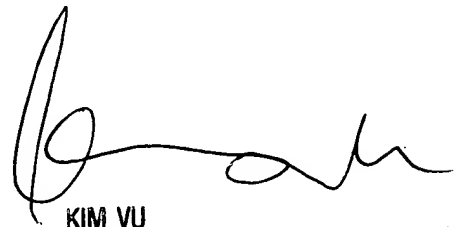
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Beemnet W. Dada whose telephone number is (571) 272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Beemnet Dada

July 22, 2005



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100